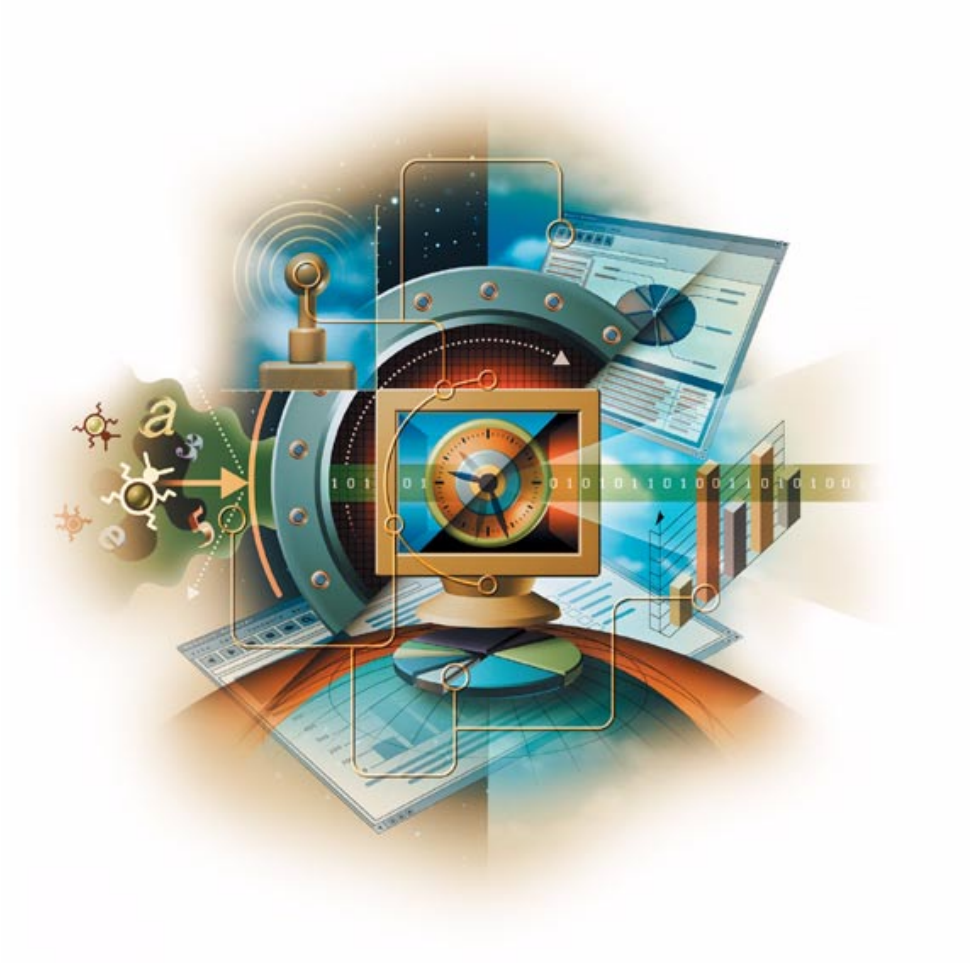
Installation Guide
Revision 1.0

# McAfee Desktop Firewall™

version 8.0



McAfee SECURITY

## COPYRIGHT

© 2003 Networks Associates Technology, Inc. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Networks Associates Technology, Inc., or its suppliers or affiliate companies. To obtain this permission, write to the attention of the Network Associates legal department at: 5000 Headquarters Drive, Plano, Texas 75024, or call +1-972-308-9960.

## TRADEMARK ATTRIBUTIONS

*Active Firewall, Active Security, Active Security (in Katakana), ActiveHelp, ActiveShield, AntiVirus Anyware and design, AVERT, Bomb Shelter, Certified Network Expert, Clean-Up, CleanUp Wizard, CNX, CNX Certification Certified Network Expert and design, Covert, Design (stylized N), Disk Minder, Distributed Sniffer System, Distributed Sniffer System (in Katakana), Dr Solomon's, Dr Solomon's label, Enterprise SecureCast, Enterprise SecureCast (in Katakana), ePolicy Orchestrator, Event Orchestrator (in Katakana), EZ SetUp, First Aid, ForceField, GMT, GroupShield, GroupShield (in Katakana), Guard Dog, HelpDesk, HomeGuard, Hunter, LANGuru, LANGuru (in Katakana), M and design, Magic Solutions, Magic Solutions (in Katakana), Magic University, MagicSpy, MagicTree, McAfee, McAfee (in Katakana), McAfee and design, McAfee.com, MultiMedia Cloaking, Net Tools, Net Tools (in Katakana), NetCrypto, NetOctopus, NetScan, NetShield, NetStalker, Network Associates, Network Policy Orchestrator, NetXray, NotesGuard, nPO, Nuts & Bolts, Oil Change, PC Medic, PCNotary, PortalShield, Powered by SpamAssassin, PrimeSupport, Recoverkey, Recoverkey – International, Registry Wizard, Remote Desktop, ReportMagic, RingFence, Router PM, Safe & Sound, SalesMagic, SecureCast, Service Level Manager, ServiceMagic, SmartDesk, Sniffer, Sniffer (in Hangul), SpamKiller, SpamAssassin, Stalker, SupportMagic, ThreatScan, TIS, TMEG, Total Network Security, Total Network Visibility, Total Network Visibility (in Katakana), Total Service Desk, Total Virus Defense, Trusted Mail, UnInstaller, Virex, Virus Forum, ViruScan, VirusScan, WebScan, WebShield, WebShield (in Katakana), WebSniffer, WebStalker, WebWall, Who's Watching Your Network, WinGauge, Your E-Business Defender, ZAC 2000, Zip Manager* are registered trademarks or trademarks of Network Associates, Inc. and/or its affiliates in the US and/or other countries. Sniffer® brand products are made only by Network Associates, Inc. All other registered and unregistered trademarks in this document are the sole property of their respective owners.

This product includes or may include software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes or may include cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes or may include some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar Free Software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires that for any software covered under the GPL which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any such software covered under the GPL, the source code is made available on this CD. If any Free Software licenses require that Network Associates provide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein.

## LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEB SITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO NETWORK ASSOCIATES OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Issued June 2003 / McAfee Desktop Firewall™ software version 8.0

DOCUMENT BUILD # DBN 002-EN

# Contents


**Preface** . . . . . 5

Audience . . . . . 5
Conventions . . . . . 6
Getting information . . . . . 7
Contacting McAfee Security & Network Associates . . . . . 8

**1 Introducing Desktop Firewall** . . . . . 9

What Desktop Firewall does . . . . . 9
Desktop Firewall components . . . . . 9
    Stand-alone version . . . . . 9
    ePolicy Orchestrator version . . . . . 10

**2 Installing the Software (Stand-alone Version)** . . . . . 11

Installation overview . . . . . 11
Before you install . . . . . 12
    Incompatible software . . . . . 12
    System requirements . . . . . 12
Installing the software . . . . . 13
Removing the software . . . . . 14

**3 Installing the Software via ePolicy Orchestrator** . . . . . 15

Installation overview . . . . . 15
Deployment recommendations . . . . . 16
System requirements . . . . . 17
    Console and server requirements . . . . . 17
    Client requirements . . . . . 18
        Minimum system requirements . . . . . 18
        Incompatible software . . . . . 19

Installing the software . . . . . 19
Running the McAfee Desktop Firewall ePO Update software . . . . . 19
Adding the Desktop Firewall client software to ePolicy Orchestrator . . . . . 20
Adding the .NAP file to ePolicy Orchestrator . . . . . 20
Adding the package file to ePolicy Orchestrator . . . . . 20
Deploying Desktop Firewall to other computers . . . . . 21
Configuring the Deployment task for Desktop Firewall . . . . . 21
Creating a deployment schedule for the Deployment task . . . . . 22
Removing Desktop Firewall . . . . . 23
Removing Desktop Firewall from client computers . . . . . 23
Removing the Desktop Firewall .NAP file from the Repository . . . . . 24
Removing the Desktop Firewall package file from the Repository . . . . . 24
Uninstalling the McAfee Desktop Firewall ePO Update software . . . . . 25

# Preface

This guide introduces McAfee Desktop Firewall™ software version 8.0, and provides the following information:

- Overview of the product.
- Detailed instructions for installing the software.

## Audience

This information is intended primarily for two audiences:

- Network administrators who are responsible for their company's anti-virus and security program.
- Users with some responsibility for configuring and using the software on their own workstations.

# Conventions

This guide uses the following conventions:

**Bold**

All words from the user interface, including options, menus, buttons, and dialog box names.

**Example**

Type the **User name** and **Password** of the desired account.

`Courier`

Text that represents something the user types exactly; for example, a command at the system prompt.

**Example**

To enable the agent, run this command line on the client computer:

```
FRMINST.EXE /INSTALL=AGENT /SITEINFO=C:\TEMP\SITELIST.XML
```

*Italic*

Names of product manuals and topics (headings) within the manuals; emphasis; introducing a new term.

**Example**

Refer to the *Desktop Firewall Product Guide* for more information.

<TERM>

Angle brackets enclose a generic term.

**Example**

In the console tree under **ePolicy Orchestrator**, right-click <SERVER>.

**NOTE**

Supplemental information; for example, an alternate method of executing the same command.

**WARNING**

Important advice to protect a user, computer system, enterprise, software installation, or data.

# Getting information

| | |
|---|---|
| **Installation Guide *†** | (This guide.)<br>System requirements and instructions for installing and starting the software.<br>*Desktop Firewall 8.0 Installation Guide* |
| **Product Guide *** | Product introduction and features, detailed instructions for configuring the software, information on deployment, recurring tasks, and operating procedures.<br>*Desktop Firewall 8.0 Product Guide* |
| **Help §** | High-level and detailed information on configuring and using the software.<br>*What's This?* field-level help. |
| **Release Notes ‡** | *ReadMe.* Product information, resolved issues, any known issues, and last-minute additions or changes to the product or its documentation. |
| **Contacts ‡** | Contact information for McAfee Security and Network Associates services and resources: technical support, customer service, AVERT (Anti-Virus Emergency Response Team), beta program, and training. This file also includes phone numbers, street addresses, web addresses, and fax numbers for Network Associates offices in the United States and around the world. |

* An Adobe Acrobat .PDF file on the product CD or the McAfee Security download site.

† A printed manual that accompanies the product CD.

‡ Text files included with the software application and on the product CD.

§ Help accessed from the software application: Help menu and/or Help button for page-level help; *What's This?* button for field-level help.

# Contacting McAfee Security & Network Associates

| | |
|---|---|
| **Technical Support** | |
| Home Page | http://www.nai.com/naicommon/services/technical-support/intro.asp |
| KnowledgeBase Search | https://knowledgemap.nai.com/phpclient/Homepage.aspx |
| PrimeSupport Service Portal * | http://mysupport.nai.com |
| **McAfee Beta Program** | http://www.mcafeeb2b.com/beta/ |
| **AVERT Anti-Virus Emergency Response Team** | |
| Home Page | http://www.mcafeeb2b.com/naicommon/avert/default.asp |
| Virus Information Library | http://vil.nai.com |
| Submit a Sample | https://www.webimmune.net/default.asp |
| **Download Site** | |
| Home Page | http://www.mcafeeb2b.com/naicommon/download/ |
| DAT File and Engine Updates | http://www.mcafeeb2b.com/naicommon/download/dats/find.asp |
| | ftp://ftp.nai.com/pub/antivirus/datfiles/4.x |
| Product Upgrades * | http://www.mcafeeb2b.com/naicommon/download/upgrade/login.asp |
| **Training** | |
| On-Site Training | http://www.mcafeeb2b.com/services/mcafee-training/default.asp |
| McAfee Security University | http://www.mcafeeb2b.com/services/mcafeesecurityu.asp |
| **Network Associates Customer Service** | |
| E-mail | services_corporate_division@nai.com |
| Web | http://www.nai.com |
| | http://www.mcafeeb2b.com |
| US, Canada, and Latin America toll-free: | |
| Phone | **+1-888-VIRUS NO** or **+1-888-847-8766** |
| | Monday – Friday, 8 a.m. – 8 p.m., Central Time |

For additional information on contacting Network Associates and McAfee Security— including toll-free numbers for other geographic areas — see the Contact file that accompanies this product release.

* Login credentials required.

# Introducing Desktop Firewall 1

This section introduces the Desktop Firewall software, including:

- What Desktop Firewall does.
- The Desktop Firewall components.

## What Desktop Firewall does

The Desktop Firewall software provides security for individual computers. It protects computers from external threats (like hackers) and from internal threats (like some viruses). It secures computers using several features, including:

- **A firewall** that inspects incoming and outgoing network traffic, and either blocks it or allows it based on rules that you set up.
- **An application monitoring system**, which monitors the applications you use and prevents those you specify from starting, or from binding themselves to other programs.
- **An intrusion detection system (IDS)** that scans traffic destined for your computer and identifies any potential attacks on your system.
- **An activity log** that records information about Desktop Firewall actions. You can use this log to troubleshoot problems, or review past activities.

You can use all of these features together, or just those features that you need.

## Desktop Firewall components

The Desktop Firewall software comes in two versions — a stand-alone version and an ePolicy Orchestrator (ePO) version.

### Stand-alone version

The stand-alone version of Desktop Firewall runs on a single computer. You configure the software directly. This version is ideal for individual users or small corporate networks.

For more information on the stand-alone version of Desktop Firewall and its features, see the *Desktop Firewall Product Guide*.

# ePolicy Orchestrator version

The ePolicy Orchestrator (ePO) version of Desktop Firewall is designed for enterprise users. McAfee ePolicy Orchestrator is a software management product that you purchase separately. Using ePolicy Orchestrator, you can store the Desktop Firewall software in a central **Repository**. Once the software is in the **Repository**, you can deploy it at any time to any number of ePO-managed computers.

ePolicy Orchestrator lets you configure, distribute, and manage Desktop Firewall for all your network users, from a single point — the ePO console. It also gives you access to more features. The ePolicy Orchestrator version of Desktop Firewall includes all the features of the stand-alone version, plus additional features such as the ability to:

- Quarantine systems that don't have up-to-date ePO policies.
- Create reports.
- Monitor users' firewall and application rules remotely.

Fore more information on the ePolicy Orchestrator version of Desktop Firewall and its features, see the *Desktop Firewall Product Guide*.

# Installing the Software (Stand-alone Version) 2

This section provides:

- An overview of how to install and deploy the stand-alone version of Desktop Firewall.
- A list of system requirements.
- Instructions for installing the software.
- Instructions for removing the software.

## Installation overview

To install the Desktop Firewall software, you must:

1. Check to see if your computer uses PGP software, specifically PGPadmin or PGPvpn components.

   See *Incompatible software* on page 12.

2. Verify that your computer meets the minimum system requirements for running Desktop Firewall.

   See *System requirements* on page 12.

3. Download the Desktop Firewall files from the McAfee Security web site, or insert the product CD into your computer's CD-ROM drive.
4. Review the Desktop Firewall Readme file for additional installation information.
5. Run the Desktop Firewall installation program.

   See *Installing the software* on page 13.

6. Restart your computer.

If you need to remove the Desktop Firewall software from your computer, follow the instructions in *Removing the software* on page 14.

# Before you install

Before you install Desktop Firewall, make certain that:

- Your computer does not use products that are incompatible with Desktop Firewall (see *Incompatible software*).
- Your computer meets the minimum system requirements for running Desktop Firewall (see *System requirements*).

## Incompatible software

The Desktop Firewall software is not compatible with the PGPadmin and PGPvpn components of the following software suites:

- PGP Desktop Security, version 7.0 or later.
- PGP Corporate Desktop, version 7.1 or later.
- PGPfire Personal Firewall/IDS, version 7.1 or later.

You must remove the PGPadmin and PGPvpn components if you plan to install and use Desktop Firewall.

## System requirements

Before you install Desktop Firewall, verify that your computer satisfies the software's minimum system requirements:

- An Intel Pentium 166MHz processor, or faster.
- A monitor offering a minimum display resolution of 800 X 600 (1024 X 768 recommended).
- One of the following amounts of RAM (depending on your operating system):
  - A minimum of 32MB of RAM for Windows 98 SE or Windows Me.
  - A minimum of 64MB of RAM for Windows NT, Windows 2000, and Windows XP.
- A minimum of 32MB hard disk space.

- One of the following Microsoft operating systems:
  - Windows 98 SE (Second Edition).
  - Windows NT Workstation 4.0, with Service Pack 6 or later.
  - Windows NT Server 4.0, with Service Pack 6 or later.
  - Windows 2000 Professional, with Service Pack 2.
  - Windows 2000 Server, with Service Pack 2.
  - Windows 2000 Advanced Server, with Service Pack 2.
  - Windows ME (Millennium Edition).
  - Windows XP Home.
  - Windows XP Professional.
- Microsoft Internet Explorer version 5.5, with Service Pack 2 or later.

**NOTE**
These are the minimum system requirements. McAfee Security recommends that you always use the latest service packs, and that you install all available security HotFixes before installing Desktop Firewall.

# Installing the software

See *Before you install* on page 12 for software compatibility information before you install Desktop Firewall.

1. Do one of the following:
   - If installing from the product CD, insert it into the CD-ROM drive of your computer.
   - If using files downloaded from the McAfee Security download site, continue to Step 2.
2. In Windows, click **Start**, then select **Run**.

   The **Run** dialog box appears.
3. Browse to the location of your Desktop Firewall SETUP.EXE file, then click **OK**.

   The default location for this file is \PRODUCTS\DESKTOP FIREWALL\SETUP.EXE, either on your installation CD or in the folder where you saved your download files.

   Your Desktop Firewall software installation begins.

4 Follow the installation wizard's prompts to continue installing the product.

5 When the installation finishes, click **Finish** to restart your computer and start Desktop Firewall.

> **NOTE**
> If you deselect the **Yes, I want to restart my computer now** checkbox, you must restart your computer before Desktop Firewall can secure any communications.

# Removing the software

1 In Windows, click **Start**, then select **Settings**.

2 Select **Control Panel**, then select **Add/Remove Programs**.

The **Add/Remove Programs** dialog box appears.

3 Select **McAfee Desktop Firewall 8.0** from the list, then click **Change/Remove**.

A welcome dialog box appears.

4 Select **Remove** to uninstall the Desktop Firewall software, then click **Next**.

5 Click **Yes** to verify that you want to remove the application.

6 Click **Finish** to restart the computer and finish removing Desktop Firewall.

> **NOTE**
> If you select the **No, I will restart my computer later** checkbox, Desktop Firewall will not be completely removed until you restart your computer.

# Installing the Software via ePolicy Orchestrator 3

This section provides:

- An overview of how to install and deploy Desktop Firewall using ePolicy Orchestrator version 3.0.
- A suggested deployment scenario.
- A list of system requirements.
- Instructions for installing the software.
- Instructions for removing the software.

## Installation overview

To deploy and manage Desktop Firewall software using ePolicy Orchestrator, follow these steps (each of which is a procedure described in this section or in the ePolicy Orchestrator documentation):

1 Install ePolicy Orchestrator and a database.

Verify that your ePolicy Orchestrator server meets the minimum system requirements for running Desktop Firewall. See *Console and server requirements* on page 17.

See the ePolicy Orchestrator documentation for installation instructions.

2 Log on to ePolicy Orchestrator and set up its **Repository**. You must add any sites, groups, or individual computers to which you plan to deploy Desktop Firewall.

3 Deploy ePolicy Orchestrator agents to these computers.

You can skip this procedure if you already have ePolicy Orchestrator agents installed on these computers.

See the ePolicy Orchestrator documentation for agent deployment instructions.

4 On your ePolicy Orchestrator server, run the **McAfee Desktop Firewall ePO Update** software.

See *Running the McAfee Desktop Firewall ePO Update software* on page 19.

5 Add the Desktop Firewall client software (.NAP and .PKG files) to the ePolicy Orchestrator **Repository**.

See *Adding the Desktop Firewall client software to ePolicy Orchestrator* on page 20.

6 Verify that your target Desktop Firewall computers meet the minimum system requirements for Desktop Firewall.

See *Client requirements* on page 18.

7 Configure the rules and other Desktop Firewall settings that you want to deploy.

See the *Desktop Firewall Product Guide* for information.

8 Deploy the Desktop Firewall client software to each of your target computers.

See *Deploying Desktop Firewall to other computers* on page 21.

# Deployment recommendations

Always develop a basic set of rules for Desktop Firewall before you deploy the product on a large scale. You can create a common rule set using the following approach, which involves working with a small test group before deploying the Desktop Firewall software to the rest of the network:

1 Using ePolicy Orchestrator, deploy the Desktop Firewall software to an administrator's computer.

2 Put the deployed product in **Learn Mode** (for both the firewall and for application monitoring).

Use **Audit Learn Mode** if you do not want to respond to regular **Learn Mode** alerts. See the **Desktop Firewall Product Guide** for more information.

3 Use this computer normally for at least a week.

**Learn Mode** continually adds rules that are appropriate to your network.

4 After a week, review the new firewall rules, application monitoring rules, and blocked hosts in Desktop Firewall. If necessary:

- Delete any rules that are not appropriate for general users.
- Add any additional rules that you need.

5 Using ePolicy Orchestrator, define this configuration as the common configuration for all future Desktop Firewall software deployments.

6 Deploy Desktop Firewall to a larger test group (ten to twenty users is ideal), and put the products in **Learn Mode** or **Audit Learn Mode**.

   This group of users will test your new Desktop Firewall configuration. Check their rule lists regularly for any new learned rules, and add these to the common configuration if appropriate.

   When the test group software operates for a week without learning any new and relevant rules, your common configuration is ready for general release.

7 Disable **Learn Mode** for all your test users, and for the common Desktop Firewall configuration.

8 Deploy the Desktop Firewall software to all your remaining network computers.

9 Using ePolicy Orchestrator, generate reports to confirm that Desktop Firewall was properly deployed to all the required computers.

# System requirements

Before you install Desktop Firewall, make certain that your hardware meets the minimum requirements to run the software. Desktop Firewall consists of two main components, each with different system requirements:

- The ePO-based console and server.
- The deployed client(s).

You generally install both the console and server on a single ePolicy Orchestrator server. This ePolicy Orchestrator server must meet the minimum requirements specified in *Console and server requirements* on page 17.

Once you finish integrating the server and console with ePolicy Orchestrator, you can use the software to deploy Desktop Firewall clients to computers managed by ePO. Each of these target computers must meet the minimum system requirements specified in *Client requirements* on page 18.

## Console and server requirements

You install the console and server components on an ePolicy Orchestrator server that:

- Runs ePolicy Orchestrator version 3.0.
- Meets the minimum system requirements for this version.

# Client requirements

Before you use ePolicy Orchestrator to deploy Desktop Firewall clients, you must do the following:

- Make certain that each target computer satisfies the minimum system requirements.
- Uninstall any incompatible software from each target computer.

## Minimum system requirements

- An Intel Pentium 166MHz processor, or faster.
- A monitor offering a minimum display resolution of 800 X 600 (1024 X 768 recommended).
- A minimum of 64MB of RAM.
- A minimum of 32MB hard disk space.
- One of the following Microsoft operating systems:
  - Windows 98 SE (Second Edition).
  - Windows NT Workstation 4.0, with Service Pack 6 or later.
  - Windows NT Server 4.0, with Service Pack 6 or later.
  - Windows 2000 Professional, with Service Pack 2.
  - Windows 2000 Server, with Service Pack 2.
  - Windows 2000 Advanced Server, with Service Pack 2.
  - Windows Me (Millennium Edition).
  - Windows XP Home Edition.
  - Windows XP Professional.
- Microsoft Internet Explorer version 5.5, with Service Pack 2 or later.

**NOTE**
These are the minimum system requirements. McAfee Security recommends that you always use the latest service packs, and that you install all available security HotFixes before installing Desktop Firewall.

### Incompatible software

The Desktop Firewall software is not compatible with the PGPadmin and PGPvpn components of the following software suites:

- PGP Desktop Security, version 7.0 or later.
- PGP Corporate Desktop, version 7.1 or later.
- PGPfire Personal Firewall/IDS, version 7.1 or later.

You must remove the PGPadmin and PGPvpn components if you plan to install and use Desktop Firewall.

# Installing the software

Once you verify that your computers meet the Desktop Firewall and ePolicy Orchestrator system requirements, you can install the software. To do this, you must:

1. Run the **McAfee Desktop Firewall ePO Update** application.
2. Add the Desktop Firewall .NAP file and package file to ePolicy Orchestrator.
3. Deploy the Desktop Firewall client software to the ePO-managed computers you have selected.

## Running the McAfee Desktop Firewall ePO Update software

1. Do one of the following:
   - Insert the Desktop Firewall CD into your CD-ROM drive.
   - Download Desktop Firewall from the McAfee Security web site following the instructions provided there, and unzip them to a folder on your hard disk.
2. Navigate to the **McAfee Desktop Firewall ePO Update** program file (MCAFEEFIREEPOUPDATE80.EXE) and double-click to launch it.

   This file is located in the \PRODUCTS\EPO UPDATE FOR FIREWALL\ folder.
3. When the Update wizard starts, accept the license agreement to continue.

4 Follow the remaining prompts to install the Update software.

The wizard prompts you to restart the computer when it finishes the installation.

5 Select **Yes** and click **Finish** to restart your computer.

If you use more than one ePolicy Orchestrator server, or if you use ePO remote consoles, repeat this procedure to install the Update software on each one.

# Adding the Desktop Firewall client software to ePolicy Orchestrator

To add the Desktop Firewall client software to ePolicy Orchestrator, you must add two files to the ePO **Repository**:

- A .NAP file (MCAFEEFIRE80.NAP).
- A package file (PKGCATALOG.Z).

## Adding the .NAP file to ePolicy Orchestrator

1 Start ePolicy Orchestrator and log on to the server that you want to manage.

2 If necessary, expand this server's icon (in the console tree) to see the **Repository** icon.

3 Right-click **Repository** and select **Configure Repository**.

4 When the configuration wizard starts, select **Add new software to be managed**.

5 Click **Next**.

6 Navigate to the MCAFEEFIRE80.NAP file and double-click it.

This file is located in the \PRODUCTS\DESKTOP FIREWALL FOR EPO\ folder on your Desktop Firewall installation CD, or in the folder where you extracted your Desktop Firewall download files.

ePolicy Orchestrator adds the Desktop Firewall software to the **Repository**.

## Adding the package file to ePolicy Orchestrator

1 Start ePolicy Orchestrator and log on to the server that you want to manage.

2 If necessary, expand this server's icon (in the console tree) to see the **Repository** icon.

3 Select **Repository**.

4 In the **Details** pane, locate the **AutoUpdate Tasks** area and click **Check in package**.

5 When the check-in wizard starts, click **Next** to continue.

6 Select **Products or updates**, then click **Next**.

7 When ePolicy Orchestrator prompts you for a path, click **Browse**.

8 Navigate to the package file (PKGCATALOG.Z) and double-click it.

This file is located in the \PRODUCTS\DESKTOP FIREWALL FOR EPO\ folder on your Desktop Firewall installation CD, or in the folder where you extracted your Desktop Firewall download files.

9 Click **Next**, then click **Finish** to add the package file to the **Repository**.

10 When the installation is successful, click **Close** to exit the wizard.

# Deploying Desktop Firewall to other computers

To deploy the Desktop Firewall software to other computers, you must configure and use the ePO **Deployment** task. ePolicy Orchestrator automatically creates this task for each user that you add to the **Directory**. To deploy Desktop Firewall using this task, you must:

1 Configure the task to send out the Desktop Firewall software.

2 Set up a deployment schedule for the task.

> **NOTE**
> You can only deploy Desktop Firewall to computers that you have set up in the ePolicy Orchestrator **Directory**, and that have ePO agents installed. See the ePolicy Orchestrator documentation for more details.

## Configuring the Deployment task for Desktop Firewall

1 Start ePolicy Orchestrator and log on to the server that you want to manage.

2 If necessary, expand this server's icon (in the console tree) to see the **Directory** icon.

3 Expand the **Directory** icon and navigate to the site, group, or computer to which you want to deploy the Desktop Firewall software.

4 In the details pane, click **Tasks** to display that tab.

ePolicy Orchestrator lists all the tasks for this site, group, or computer.

5 Right-click the **Deployment** task, then select **Edit Task**.

The **ePolicy Orchestrator Scheduler** dialog box appears.

6 Click **Task** to display that tab.

7 Click **Settings**.

The **Task Settings** dialog box appears.

8 Deselect the **Inherit** checkbox.

9 In the **Product deployment options** list, locate **McAfee Desktop Firewall**.

10 Select **Install** from the **Action** list.

If you installed more than one language version, select the language that you want to deploy from the **Language** list.

Set any products that you do not want to remove to **Ignore**.

11 Click **OK** to return to the **ePolicy Orchestrator Scheduler** dialog box.

Now that you have configured this task to deploy Desktop Firewall, create a deployment schedule for the task.

## Creating a deployment schedule for the Deployment task

1 In the **ePolicy Orchestrator Scheduler** dialog box, click **Task** to display that tab.

2 In the **Schedule Settings** area, deselect **Inherit**.

3 Select **Enable** to make the task active.

4 Click the **Schedule** tab.

5 Deselect the **Inherit** checkbox, then set up the time when you want the Desktop Firewall software deployed.

To deploy the software immediately, select **Run Immediately** from the **Schedule Task** list.

For instructions, see the *ePolicy Orchestrator Product Guide*.

6 Click **OK**.

ePolicy Orchestrator deploys the Desktop Firewall client software to this site, group, or computer at the time you specified.

# Removing Desktop Firewall

To completely uninstall the Desktop Firewall software, you must:

- Remove Desktop Firewall from all your ePolicy Orchestrator clients.
- Delete the Desktop Firewall .NAP file from the ePolicy Orchestrator **Repository**.
- Delete the Desktop Firewall package file from the **Repository**.
- Remove the **McAfee Desktop Firewall ePO Update** software from your ePolicy Orchestrator server.

> **NOTE**
> If you have more than one ePolicy Orchestrator server, or if you use ePO remote consoles, you must uninstall the Update from each one separately.

## Removing Desktop Firewall from client computers

1. Start ePolicy Orchestrator and log on to the server that you want to manage.
2. If necessary, expand this server's icon (in the console tree) to see the **Directory** icon.
3. Expand the **Directory** icon and select the site, group, or computer that you want to remove Desktop Firewall from.
4. In ePolicy Orchestrator's details pane, click **Tasks** to display that tab.
5. Right-click the **Deployment** task, then select **Edit Task**.

   The **ePolicy Orchestrator Scheduler** dialog box appears.
6. On the **Task** tab, click **Settings**.

   The **Task Settings** dialog box appears.
7. If necessary, deselect the **Inherit** checkbox.
8. In the **Product deployment options** list, locate **McAfee Desktop Firewall**.
9. Select **Remove** from the **Action** list.

   If you installed more than one language version, select the language that you want to remove from the **Language** list.

   Set any products that you do not want to remove to **Ignore**.

10 Click **OK** to return to the **ePolicy Orchestrator Scheduler** dialog box.

11 Click **OK** to save your changes.

ePolicy Orchestrator will remove the Desktop Firewall clients at the time specified in the task. To change the task's schedule, use the procedure outlined in *Creating a deployment schedule for the Deployment task* on page 22.

## Removing the Desktop Firewall .NAP file from the Repository

1 Start ePolicy Orchestrator and log on to the server that you want to manage.

2 If necessary, expand this server's icon (in the console tree) to see the **Repository** icon.

3 Expand **Repository** to see its contents.

4 Expand **Managed Products**, and then **Windows**.

5 Right-click **McAfee Desktop Firewall** and select **Remove**.

6 Click **Yes** when ePolicy Orchestrator asks whether to remove the software.

7 Click **OK** to finish removing the Desktop Firewall software from the **Repository**.

## Removing the Desktop Firewall package file from the Repository

1 Start ePolicy Orchestrator and log on to the server that you want to manage.

2 If necessary, expand this server's icon (in the console tree) to see the **Repository** icon.

3 Select **Repository**.

4 In the **Details** pane, locate the **AutoUpdate Tasks** area and click **Manage packages**.

ePolicy Orchestrator lists all of the package files in the **Repository**.

5 Select **McAfee Desktop Firewall**.

6 Click **Delete**.

7 Click **OK** when ePolicy Orchestrator asks whether to remove the package file.

# Uninstalling the McAfee Desktop Firewall ePO Update software

1. In Windows, click **Start** and then select **Settings**.
2. Select **Control Panel**, then select **Add/Remove Programs**.

   The **Add/Remove Programs** dialog box appears.
3. Select **McAfee Desktop Firewall ePO Update** from the list, then click **Change/Remove**.
4. Click **OK** when Windows asks whether you want to remove the application.

   Windows uninstalls the Update and prompts you to restart your computer.
5. Select **Yes** and then click **Finish**.

   Your computer restarts, and Windows finishes removing the Update.

   **NOTE**
   If you select the **No, I will restart my computer later** checkbox, the Update will not be completely removed until you restart your computer.